S|3 SPECIALIZED SECURITY SERVICES

# TARGETED RISK ANALYSIS FOR PCI DSS v4

# UNDERSTANDING THE NEW RISK-BASED REQUIREMENT AND WHAT IT MEANS FOR YOUR ORGANIZATION

PCI DSS v4 introduced one of the most significant evolutions in the standard in its history, emphasizing a more flexible, risk-based approach to compliance. At the center of this shift is the **Targeted Risk Analysis (TRA)**, a requirement designed to help organizations think more strategically about how and why specific controls are implemented.

While the concept of risk-based compliance is not new, the way PCI DSS now integrates risk evaluation into its core expectations is. For many organizations, understanding when and how to perform a TRA, how to document it, and how to validate results has become a new challenge.

S3 Security helps organizations bridge that gap by turning TRA requirements into a structured, defensible, and efficient part of ongoing compliance.

# WHAT IS A TARGETED RISK ANALYSIS (TRA)?

A Targeted Risk Analysis is a formal, documented evaluation of risk for a specific control or requirement within the PCI DSS framework. Unlike a general enterprise risk assessment, a TRA is narrow in focus and tied directly to an individual PCI control where flexibility is allowed.

In simple terms, a TRA helps your organization justify how frequently a control is performed or how a customized control satisfies the intent of PCI DSS. It is not just about meeting a requirement. It is about proving that your decisions are *deliberate, informed, and proportional to risk*.

## TWO APPROACHES: STANDARD VS. CUSTOMIZED

PCI DSS v4 allows two main approaches to demonstrating compliance.

**The Standard Approach**:

- Follows PCI's prescribed controls and testing procedures.
- TRAs are used primarily to determine control frequency (for example, how often vulnerability scans or password changes occur).
- These are shorter, more procedural, and often template-based.

**The Customized Approach**:

- Offers flexibility for organizations that have unique architectures or controls that differ from PCI's predefined methods.
- TRAs under this approach are deeper and require full justification of how a control meets the intent of PCI DSS.
- Includes detailed documentation of threat likelihood, business justification, and executive review.

While the customized approach offers adaptability, it also demands strong internal governance and a mature understanding of risk management.

S3 Security helps organizations determine when a customized approach makes sense and when the standard approach provides more efficiency and clarity.

# WHEN AND HOW ORGANIZATIONS MUST PERFORM TRAS

TRAs are required whenever PCI DSS allows entities to define their own control frequency or when they adopt a customized approach.

## COMMON EXAMPLES INCLUDE:

- Setting periodic scan or monitoring intervals.
- Determining how often malware scans or user access reviews are performed.
- Justifying how a custom control satisfies the intent of a standard requirement.

## A TRA MUST BE CONDUCTED:

- At least annually or whenever significant environmental or operational changes occur.
- Using a consistent, documented methodology.
- Reviewed and approved by relevant stakeholders – including your QSA.

S3 Security's TRA methodology aligns with PCI SSC guidance while tailoring analysis depth and structure to your organization's maturity level and environment complexity.

# HOW TO JUSTIFY CONTROL FREQUENCY, SCOPE AND RESIDUAL RISK

The core of a strong TRA lies in justification; demonstrating that your chosen frequency, method, and/or control scope is backed by measurable reasoning. Each TRA should include:

- **Objective**
  Which control or activity is being analyzed and why.
- **Asset and Threat Identification**
  Which systems or data are affected, and what could go wrong.
- **Impact and Likelihood**
  Severity and probability of each risk scenario.
- **Chosen Frequency or Control Justification**
  Why this cadence or approach sufficiently reduces risk.
- **Residual Risk**
  What remains after controls are applied, and why it is acceptable.
- **Review and Signoff**
  Documentation of management review and QSA verification.

S3 Security helps clients develop reusable TRA templates that satisfy these documentation requirements and withstand QSA review.

# COMMON PITFALLS AND BEST PRACTICES

Many organizations approach TRAs with good intentions but fall short in consistency or clarity. Common mistakes include:

- Copying generic templates without tailoring them to specific environments.
- Failing to document how frequency decisions were reached.
- Neglecting to review TRAs annually or after significant changes.
- Treating TRAs as paperwork instead of an active risk management exercise.

## BEST PRACTICES INCLUDE:

- Starting small by focusing first on high-priority controls such as vulnerability scanning or access reviews.
- Keeping it measurable by using data, not assumptions, to justify decisions.
- Building annual TRA review into your PCI compliance calendar.
- Involving leadership so business owners understand and approve risk-based decisions.


## THE BUSINESS VALUE OF TRA MATURITY

Mature TRAs do more than satisfy PCI DSS. They enhance overall security governance. Organizations with well-documented TRAs:

- Demonstrate stronger due diligence during audits.
- Reduce repetitive compliance work by reusing validated templates.
- Gain better visibility into operational risk.
- Empower management to make smarter, risk-based decisions.

Over time, TRA maturity leads to reduced friction between security and compliance teams, faster audits, and greater confidence in control performance.

# HOW S3 SECURITY CAN HELP

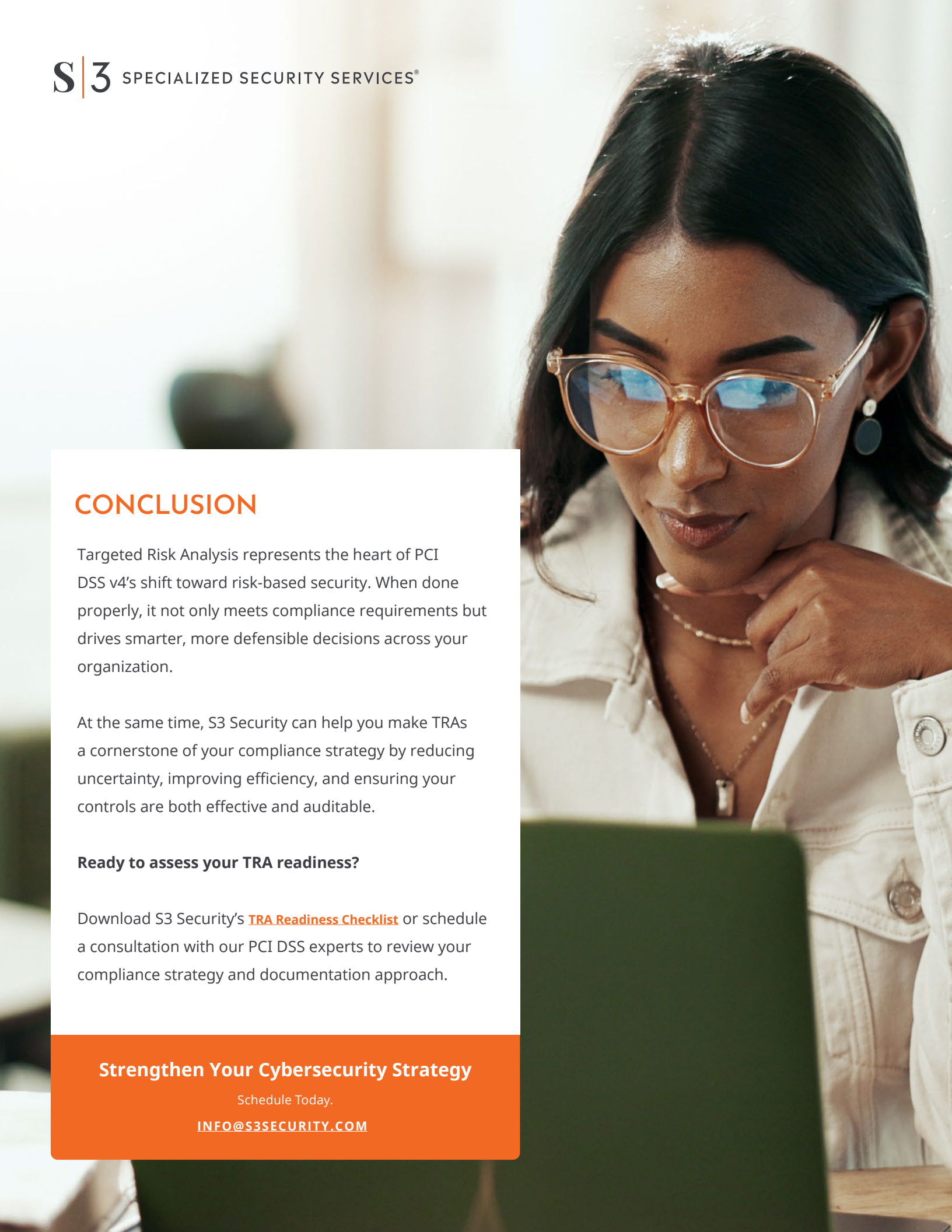
S3 Security supports organizations through every step of the Targeted Risk Analysis process. Our PCI Qualified Security Assessors bring decades of combined experience to the process of helping clients build, document, and maintain risk-based controls that align with PCI DSS v4.

Our services include:

- TRA methodology design and documentation templates.
- Training and workshops for compliance and security teams.
- TRA validation and annual review support.
- Integration of TRA processes into ongoing compliance programs.

Every engagement is led by a senior-level assessor. There are no junior resources, no hand-offs, and no unnecessary complexity. S3 Security provides practical, expert guidance designed to simplify compliance and strengthen your security program.

S|3 SPECIALIZED SECURITY SERVICES®



## CONCLUSION

Targeted Risk Analysis represents the heart of PCI DSS v4's shift toward risk-based security. When done properly, it not only meets compliance requirements but drives smarter, more defensible decisions across your organization.

At the same time, S3 Security can help you make TRAs a cornerstone of your compliance strategy by reducing uncertainty, improving efficiency, and ensuring your controls are both effective and auditable.

**Ready to assess your TRA readiness?**

Download S3 Security's **TRA Readiness Checklist** or schedule a consultation with our PCI DSS experts to review your compliance strategy and documentation approach.

**Strengthen Your Cybersecurity Strategy**

Schedule Today.

**INFO@S3SECURITY.COM**